

Exhibit 5

DELL CAMERON

SECURITY MAR 8, 2023 2:45 PM

The FBI Just Admitted It Bought US Location Data

Rather than obtaining a warrant, the bureau purchased sensitive data—a controversial practice that privacy advocates say is deeply problematic.



FBI director Christopher Wray disclosed the purchase of location data during a Senate hearing on Wednesday, March 8. PHOTOGRAPH: TOM WILLIAMS/GETTY IMAGES

 SAVE

THE UNITED STATES Federal Bureau of Investigation has acknowledged for the first time that it purchased US location data rather than obtaining a warrant. While the practice of buying people’s location data has grown increasingly common since the US Supreme Court reined in the government’s ability to warrantlessly track Americans’ phones nearly five years ago, the FBI had not previously revealed ever making such purchases.

The disclosure came today during a US Senate hearing on global threats attended by five of the nation’s intelligence chiefs. Senator Ron Wyden, an Oregon Democrat, put the question of the bureau’s use of commercial data to its director, Christopher Wray: “Does the FBI purchase US phone-geolocation information?” Wray said his agency was not currently doing so, but he acknowledged that it had in the past. He also limited his response to data companies gathered specifically for advertising purposes.

ADVERTISEMENT





“To my knowledge, we do not currently purchase commercial database information that includes location data derived from internet advertising,” Wray said. “I understand that we previously—as in the past—purchased some such information for a specific national security pilot project. But that’s not been active for some time.” He added that the bureau now relies on a “court-authorized process” to obtain location data from companies.

It’s not immediately clear whether Wray was referring to a warrant—that is, an order signed by a judge who is reasonably convinced that a crime has occurred—or another legal device. Nor did Wray indicate what motivated the FBI to end the practice.

In its landmark *Carpenter v. United States* decision, the Supreme Court held that government agencies accessing historical location data without a warrant were violating the Fourth Amendment’s guarantee against unreasonable searches. But the ruling was narrowly construed. Privacy advocates say the decision left open a glaring loophole that allows the government to simply purchase whatever it cannot otherwise legally obtain. US Customs and Border Protection (CBP) and the Defense Intelligence Agency are among the list of federal agencies known to have taken advantage of this loophole.

The Department of Homeland Security, for one, is reported to have purchased the geolocations of millions of Americans from private marketing firms. In that instance, the data were derived from a range of deceptively benign sources, such as mobile games and weather apps. Beyond the federal government, state and local authorities have been known to acquire software that feeds off cellphone-tracking data. Asked during the Senate hearing whether the FBI would pick up the practice of purchasing location data again, Wray replied: “We have no plans to change that, at the current time.”

Sean Vitka, a policy attorney at Demand Progress, a nonprofit focused on national security and privacy reform, says the FBI needs to be more forthcoming about the

purchases, calling Wray's admission "horrifying" in its implications. "The public needs to know who gave the go-ahead for this purchase, why, and what other agencies have done or are trying to do the same," he says, adding that Congress should also move to ban the practice entirely.

US lawmakers have long failed in their attempts to pass a comprehensive privacy law, and most of the bills put forth have purposely avoided the government's own acquisition of US residents' personal data. The American Data Privacy and Protection Act (ADPPA) introduced last year, for instance, contains exemptions for all law enforcement agencies and any company "collecting, processing, or transferring" data on their behalf. Several bills authored by Wyden and other lawmakers have attempted to tackle the issue head-on. The Geolocation Privacy and Surveillance Act, for example, has been reintroduced in Congress numerous times since 2011 but has failed to receive a vote.

See What's Next in Tech With the Fast Forward Newsletter

A weekly dispatch from the future by Will Knight, exploring AI advances and other technology set to change our lives. Delivered every Thursday.

Your email

Enter your email




SUBMIT

By signing up you agree to our [User Agreement](#) (including the [class action waiver and arbitration provisions](#)), our [Privacy Policy & Cookie Statement](#) and to receive marketing and account-related emails from WIRED. You can unsubscribe at any time.

Last month, Demand Progress joined a coalition of privacy groups in urging the head of the US financial protection bureau to use the Fair Credit Report Act (FCRA)—the nation's first major privacy law—against data brokers commodifying Americans' information without their consent. Attorneys who signed on to the campaign, from organizations such as the National Consumer Law Center and Just Futures Law, said the privacy violations inherent to the data broker industry disproportionately impact society's most vulnerable, interfering with their ability to obtain jobs, housing, and government benefits.

While the 21st century's privacy problems may have been beyond the imaginings of the FCRA's authors 50 years ago, modern injustices tied to the sale of personal data may, they argue, still fall under its purview.

Get More From WIRED

-  Get the best stories from WIRED's iconic archive in your inbox
-  Our new podcast wants you to *Have a Nice Future*
- The real reason Steph Curry is so damn good
- Google's search box changed the meaning of information
- For the love of God, stop microwaving plastic
- Critical Role lays out the next era in tabletop games
- Should you buy an active chair? I tested some—and talked to the experts
-  See if you take a shine to our picks for the best sunglasses and sun protection

Dell Cameron is a Texas-based privacy, policy, and security reporter. Prior to joining WIRED, he was a staff reporter at the Daily Dot and senior reporter at Gizmodo.

SENIOR REPORTER, POLITICS AND POLICY 

TOPICS SURVEILLANCE PRIVACY FBI

MORE FROM WIRED